AMENDMENTS TO THE CLAIMS

1-10. (Canceled)

11. (Currently amended) ~~The~~ In a system comprising an application, a framework, and an implementation class which provides an implementation for a particular service, a method ~~of claim 1,~~ performed by the framework, comprising:

receiving a request from an application for a customized implementation of a particular service;

instantiating an implementation class which provides an implementation for the particular service to give rise to an implementation instance;

determining a set of zero or more restrictions to be imposed on said customized implementation;

instantiating a wrapper class to give rise to a wrapper instance, said wrapper instance comprising enforcement logic for enforcing said restrictions;

encapsulating said implementation instance and said restrictions within said wrapper instance; and

providing said wrapper instance to the application as said customized implementation;

wherein said wrapper instance comprises one or more invocable methods, wherein said implementation instance comprises one or more invocable methods, and wherein encapsulating comprises:

mapping the one or more invocable methods of said wrapper instance to the one or more invocable methods of said implementation instance.

12. (Currently amended) The method of claim 11, wherein instantiating the implementation class comprises:

determining whether the implementation class is authentic; and

in response to a determination that the implementation class is authentic, instantiating the implementation class to give rise to said implementation instance.

13. (Original) The method of claim 12, wherein the implementation class has a digital signature associated therewith, and wherein determining whether the implementation class is authentic comprises:

verifying said digital signature.

Cont B1

14. (Original) The method of claim 12, wherein the implementation class authenticates the framework prior to giving rise to said implementation instance.

15. (Currently amended) The method of claim 11, wherein determining the set of zero or more restrictions comprises:

accessing information specifying one or more limitations; and

processing said limitations to derive said restrictions.

16. (Original) The method of claim 15, wherein the particular service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations.

17. (Original) The method of claim 16, wherein said default encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

18. (Currently amended) The method of claim 11, wherein determining the set of zero or more restrictions comprises:

accessing information specifying one or more limitations;

determining permissions, if any, granted to the application; and

reconciling said limitations and said permissions to derive said restrictions.

Cont B1

19. (Original) The method of claim 18, wherein said limitations and said permissions are reconciled to derive restrictions which are least restrictive.

20. (Original) The method of claim 18, wherein the particular service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations, and a set of zero or more exempt encryption limitations which apply when one or more exemption mechanisms are implemented.

21. (Original) The method of claim 20, wherein said default encryption limitations and said exempt encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

22. (Original) The method of claim 20, wherein reconciling said limitations and said permissions comprises:

determining whether the application has been granted any permissions; and

in response to a determination that the application has not been granted any permissions, deriving said restrictions from said set of default encryption limitations.

23. (Original) The method of claim 20, wherein reconciling said limitations and said permissions comprises:

determining whether the application has been granted any permissions which require implementation of a particular exemption mechanism;

in response to a determination that the application has been granted a permission which requires implementation of a particular exemption mechanism, determining whether said exempt encryption limitations allow said particular exemption mechanism to be implemented; and

in response to a determination that said exempt encryption limitations allow said particular exemption mechanism to be implemented, deriving said restrictions from said set of exempt encryption limitations.

24-33. (Canceled)

34. (Currently amended) ~~The~~ In a system comprising an application and an implementation class which provides an implementation for a particular service, a framework ~~of claim 24,~~ comprising:

a mechanism for receiving a request from an application for a customized implementation of a particular service;

a mechanism for instantiating an implementation class which provides an implementation for the particular service to give rise to an implementation instance;

a mechanism for determining a set of zero or more restrictions to be imposed on said customized implementation;

a mechanism for instantiating a wrapper class to give rise to a wrapper instance, said wrapper instance comprising enforcement logic for enforcing said restrictions;

a mechanism for encapsulating said implementation instance and said restrictions within said wrapper instance; and

a mechanism for providing said wrapper instance to the application as said customized implementation;

wherein said wrapper instance comprises one or more invocable methods, wherein said implementation instance comprises one or more invocable methods, and wherein the mechanism for encapsulating comprises:

a mechanism for mapping the one or more invocable methods of said wrapper instance to the one or more invocable methods of said implementation instance.

35. (Currently amended) The framework of claim ~~24~~34, wherein the mechanism for instantiating the implementation class comprises:

a mechanism for determining whether the implementation class is authentic; and

a mechanism for instantiating, in response to a determination that the implementation class is authentic, the implementation class to give rise to said implementation instance.

36. (Original) The framework of claim 35, wherein the implementation class has a digital signature associated therewith, and wherein the mechanism for determining whether the implementation class is authentic comprises:

a mechanism for verifying said digital signature.

37. (Original) The framework of claim 35, wherein the implementation class authenticates the framework prior to giving rise to said implementation instance.

38. (Currently amended) The framework of claim ~~24~~34, wherein the mechanism for determining the set of zero or more restrictions comprises:

a mechanism for accessing information specifying one or more limitations; and

a mechanism for processing said limitations to derive said restrictions.

Cont B1

39. (Original) The framework of claim 38, wherein the particular service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations.

40. (Original) The framework of claim 39, wherein said default encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

41. (Currently amended) The framework of claim ~~24~~34, wherein the mechanism for determining the set of zero or more restrictions comprises:

a mechanism for accessing information specifying one or more limitations;

a mechanism for determining permissions, if any, granted to the application; and

a mechanism for reconciling said limitations and said permissions to derive said restrictions.

42. (Original) The framework of claim 41, wherein said limitations and said permissions are reconciled to derive restrictions which are least restrictive.

43. (Original) The framework of claim 41, wherein the particular service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations, and a set of zero or more exempt encryption limitations which apply when one or more exemption mechanisms are implemented.

Cont B1

44. (Original) The framework of claim 43, wherein said default encryption limitations and said exempt encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

45. (Original) The framework of claim 43, wherein the mechanism for reconciling said limitations and said permissions comprises:

a mechanism for determining whether the application has been granted any permissions; and

a mechanism for deriving, in response to a determination that the application has not been granted any permissions, said restrictions from said set of default encryption limitations.

46. (Original) The framework of claim 43, wherein the mechanism for reconciling said limitations and said permissions comprises:

a mechanism for determining whether the application has been granted any permissions which require implementation of a particular exemption mechanism;

a mechanism for determining, in response to a determination that the application has been granted a permission which requires implementation of a particular exemption mechanism, whether said exempt encryption limitations allow said particular exemption mechanism to be implemented; and

a mechanism for deriving, in response to a determination that said exempt encryption limitations allow said particular exemption mechanism to be implemented, said restrictions from said set of exempt encryption limitations.

47-56. (Canceled)

57. (Currently amended) ~~The~~ In a system comprising an application and an implementation class which provides an implementation for a particular service, a computer readable medium ~~of claim 47,~~ having stored thereon instructions which, when executed by one or more processors, cause the one or more processors to implement a framework which dynamically constructs a customized implementation, said computer readable medium comprising:

instructions for causing one or more processors to receive a request from an application for a customized implementation of a particular service;

instructions for causing one or more processors to instantiate an implementation class which provides an implementation for the particular service to give rise to an implementation instance;

instructions for causing one or more processors to determine a set of zero or more restrictions to be imposed on said customized implementation;

instructions for causing one or more processors to instantiate a wrapper class to give rise to a wrapper instance, said wrapper instance comprising enforcement logic for enforcing said restrictions;

instructions for causing one or more processors to encapsulate said implementation instance and said restrictions within said wrapper instance; and

instructions for causing one or more processors to provide said wrapper instance to the application as said customized implementation;

wherein said wrapper instance comprises one or more invocable methods, wherein said implementation instance comprises one or more invocable methods, and wherein the instructions for causing one or more processors to encapsulate comprises:

instructions for causing one or more processors to map the one or more invocable methods of said wrapper instance to the one or more invocable methods of said implementation instance.

58. (Currently amended) The computer readable medium of claim ~~47~~57, wherein the instructions for causing one or more processors to instantiate the implementation class comprises:

instructions for causing one or more processors to determine whether the implementation class is authentic; and

instructions for causing one or more processors to instantiate, in response to a determination that the implementation class is authentic, the implementation class to give rise to said implementation instance.

59. (Original) The computer readable medium of claim 58, wherein the implementation class has a digital signature associated therewith, and wherein the instructions for causing one or more processors to determine whether the implementation class is authentic comprises:

instructions for causing one or more processors to verify said digital signature.

Cont B1

60. (Original) The computer readable medium of claim 58, wherein the implementation class authenticates the framework prior to giving rise to said implementation instance.

61. (Currently amended) The computer readable medium of claim ~~47~~57, wherein the instructions for causing one or more processors to determine the set of zero or more restrictions comprises:

instructions for causing one or more processors to access information specifying one or more limitations; and

instructions for causing one or more processors to process said limitations to derive said restrictions.

62. (Original) The computer readable medium of claim 61, wherein the particular service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations.

63. (Original) The computer readable medium of claim 62, wherein said default encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

64. (Currently amended) The computer readable medium of claim ~~47~~57, wherein the instructions for causing one or more processors to determine the set of zero or more restrictions comprises:

instructions for causing one or more processors to access information specifying one or more limitations;

instructions for causing one or more processors to determine permissions, if any, granted to the application; and

instructions for causing one or more processors to reconcile said limitations and said permissions to derive said restrictions.

65. (Original) The computer readable medium of claim 64, wherein said limitations and said permissions are reconciled to derive restrictions which are least restrictive.

66. (Original) The computer readable medium of claim 64, wherein the particular service is an encryption/decryption service, and wherein said information comprises a set of one or more default encryption limitations, and a set of zero or more

exempt encryption limitations which apply when one or more exemption mechanisms are implemented.

67. (Original) The computer readable medium of claim 66, wherein said default encryption limitations and said exempt encryption limitations are derived by merging multiple jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

68. (Original) The computer readable medium of claim 66, wherein the instructions for causing one or more processors to reconcile said limitations and said permissions comprises:

instructions for causing one or more processors to determine whether the application has been granted any permissions; and

instructions for causing one or more processors to derive, in response to a determination that the application has not been granted any permissions, said restrictions from said set of default encryption limitations.

69. (Original) The computer readable medium of claim 66, wherein the instructions for causing one or more processors to reconcile said limitations and said permissions comprises:

instructions for causing one or more processors to determine whether the application has been granted any permissions which require implementation of a particular exemption mechanism;

instructions for causing one or more processors to determine, in response to a determination that the application has been granted a permission which requires implementation of a particular exemption mechanism, whether said exempt encryption limitations allow said particular exemption mechanism to be implemented; and

instructions for causing one or more processors to derive, in response to a determination that said exempt encryption limitations allow said particular exemption mechanism to be implemented, said restrictions from said set of exempt encryption limitations.

70. (Currently amended) The method of claim 11, wherein determining said set of zero or more restrictions includes determining a set of zero or more restrictions that are specific to said application.

71. (Previously added) The method of claim 70, wherein determining said set of zero or more restrictions that are specific to said application includes determining a set of zero or more restrictions that are customized for said application.

72. (Currently amended) The method of claim 11, wherein said set is a first set, and wherein said customized implementation is a first customized implementation, and further comprising:

receiving a request from a second application for a second customized implementation of said particular service, wherein said second customized implementation differs from said first customized implementation;

instantiating said implementation class which provides said implementation for said particular service to give rise to a second implementation instance;

determining a second set of zero or more restrictions to be imposed on said second customized implementation, wherein said second set differs from said first set;

instantiating said wrapper class to give rise to a second wrapper instance, said second wrapper instance comprising enforcement logic for enforcing said second set of zero or more restrictions;

encapsulating said second implementation instance and said second set of zero or more restrictions within said second wrapper instance; and

providing said second wrapper instance to said second application as said second customized implementation.

Cont B1

73. (Currently amended) The framework of claim ~~24~~34, wherein said mechanism for determining said set of zero or more restrictions includes a mechanism for determining a set of zero or more restrictions that are specific to said application.

74. (Previously added) The framework of claim 73, wherein said mechanism for determining said set of zero or more restrictions that are specific to said application includes a mechanism for determining a set of zero or more restrictions that are customized for said application.

75. (Currently amended) The framework of claim ~~24~~34, wherein said set is a first set, and wherein said customized implementation is a first customized implementation, and further comprising:

a mechanism for receiving a request from a second application for a second customized implementation of said particular service, wherein said second customized implementation differs from said first customized implementation;

a mechanism for instantiating said implementation class which provides said implementation for said particular service to give rise to a second implementation instance;

a mechanism for determining a second set of zero or more restrictions to be imposed on said second customized implementation, wherein said second set differs from said first set;

a mechanism for instantiating said wrapper class to give rise to a second wrapper instance, said second wrapper instance comprising enforcement logic for enforcing said second set of zero or more restrictions;

a mechanism for encapsulating said second implementation instance and said second set of zero or more restrictions within said second wrapper instance; and

a mechanism for providing said second wrapper instance to said second application as said second customized implementation.

76. (Currently amended) The computer readable medium of claim ~~49~~57, wherein said instructions for determining said set of zero or more restrictions include instructions for determining a set of zero or more restrictions that are specific to said application.

77. (Previously added) The computer readable medium of claim 76, wherein said instructions for determining said set of zero or more restrictions that are specific to

said application include instructions for determining a set of zero or more restrictions that are customized for said application.

78. (Currently amended) The computer readable medium of claim ~~49~~57, wherein said set is a first set, and wherein said customized implementation is a first customized implementation, and further comprising:

instructions for receiving a request from a second application for a second customized implementation of said particular service, wherein said second customized implementation differs from said first customized implementation;

instructions for instantiating said implementation class which provides said implementation for said particular service to give rise to a second implementation instance;

instructions for determining a second set of zero or more restrictions to be imposed on said second customized implementation, wherein said second set differs from said first set;

instructions for instantiating said wrapper class to give rise to a second wrapper instance, said second wrapper instance comprising enforcement logic for enforcing said second set of zero or more restrictions;

instructions for encapsulating said second implementation instance and said second set of zero or more restrictions within said second wrapper instance; and

instructions for providing said second wrapper instance to said second application as said second customized implementation.

79. (New) The method of claim 11, wherein said wrapper instance is invocable by the application without further interaction with the framework.

80. (New) The method of claim 11, wherein the implementation class provides an unrestricted implementation for the particular service.

81. (New) The method of claim 80, wherein the particular service is an encryption/decryption service, and wherein the unrestricted implementation provided by the implementation class is capable of using unlimited encryption/decryption parameters.

82. (New) The method of claim 81, wherein the unrestricted implementation provided by the implementation class is capable of using encryption/decryption keys of any size.

83. (New) The method of claim 11, wherein said enforcement logic enforces said restrictions on said implementation instance.

84. (New) The method of claim 83, wherein said enforcement logic enforces said restrictions on said implementation instance by:

receiving a set of desired parameters from the application;

determining whether the desired parameters exceed said restrictions; and

in response to a determination that the desired parameters exceed said restrictions, preventing said implementation instance from operating.

85. (New) The method of claim 84, wherein said enforcement logic is invoked upon initialization of said wrapper instance.

86. (New) The method of claim 11, wherein the system further comprises an exemption mechanism class which provides an implementation for a particular exemption mechanism, and wherein said method further comprises:

instantiating the exemption mechanism class to give rise to an exemption mechanism instance; and

encapsulating said exemption mechanism instance within said wrapper instance.

87. (New) The method of claim 86, wherein said enforcement logic is invoked upon initialization of said wrapper instance, and when invoked, said enforcement logic:

determines whether said exemption mechanism instance has been invoked; and

in response to a determination that said exemption mechanism instance has not been invoked, preventing said implementation instance from operating.

Cont'
B2

88. (New) The framework of claim 34, wherein said wrapper instance is invocable by the application without further interaction with the framework.

89. (New) The framework of claim 34, wherein the implementation class provides an unrestricted implementation for the particular service.

90. (New) The framework of claim 89, wherein the particular service is an encryption/decryption service, and wherein the unrestricted implementation provided by the implementation class is capable of using unlimited encryption/decryption parameters.

91. (New) The framework of claim 90, wherein the unrestricted implementation provided by the implementation class is capable of using encryption/decryption keys of any size.

92. (New) The framework of claim 34, wherein said enforcement logic enforces said restrictions on said implementation instance.

93. (New) The framework of claim 92, wherein said enforcement logic enforces said restrictions on said implementation instance by:

receiving a set of desired parameters from the application;

determining whether the desired parameters exceed said restrictions; and

in response to a determination that the desired parameters exceed said restrictions, preventing said implementation instance from operating.

Cont B2

94. (New) The framework of claim 93, wherein said enforcement logic is invoked upon initialization of said wrapper instance.

95. (New) The framework of claim 34, wherein the system further comprises an exemption mechanism class which provides an implementation for a particular exemption mechanism, and wherein said framework further comprises:

a mechanism for instantiating the exemption mechanism class to give rise to an exemption mechanism instance; and

a mechanism for encapsulating said exemption mechanism instance within said wrapper instance.

96. (New) The framework of claim 95, wherein said enforcement logic is invoked upon initialization of said wrapper instance, and when invoked, said enforcement logic:

determines whether said exemption mechanism instance has been invoked; and

in response to a determination that said exemption mechanism instance has not been invoked, preventing said implementation instance from operating.

97. (New) The computer readable medium of claim 57, wherein said wrapper instance is invocable by the application without further interaction with the framework.

98. (New) The computer readable medium of claim 57, wherein the implementation class provides an unrestricted implementation for the particular service.

Cont'd B2

99. (New) The computer readable medium of claim 98, wherein the particular service is an encryption/decryption service, and wherein the unrestricted implementation provided by the implementation class is capable of using unlimited encryption/decryption parameters.

100. (New) The computer readable medium of claim 99, wherein the unrestricted implementation provided by the implementation class is capable of using encryption/decryption keys of any size.

101. (New) The computer readable medium of claim 57, wherein said enforcement logic enforces said restrictions on said implementation instance.

102. (New) The computer readable medium of claim 101, wherein said enforcement logic enforces said restrictions on said implementation instance by:

receiving a set of desired parameters from the application;

determining whether the desired parameters exceed said restrictions; and

in response to a determination that the desired parameters exceed said restrictions, preventing said implementation instance from operating.

103. (New) The computer readable medium of claim 102, wherein said enforcement logic is invoked upon initialization of said wrapper instance.

104. (New) The computer readable medium of claim 57, wherein the system further comprises an exemption mechanism class which provides an implementation for a particular exemption mechanism, and wherein said computer readable medium further comprises:

instructions for causing one or more processors to instantiate the exemption mechanism class to give rise to an exemption mechanism instance; and

instructions for causing one or more processors to encapsulate said exemption mechanism instance within said wrapper instance.

105. (New) The computer readable medium of claim 104, wherein said enforcement logic is invoked upon initialization of said wrapper instance, and when invoked, said enforcement logic:

determines whether said exemption mechanism instance has been invoked; and

in response to a determination that said exemption mechanism instance has not been invoked, preventing said implementation instance from operating.